

(19) World Intellectual Property Organization  
International Bureau



(43) International Publication Date  
12 April 2001 (12.04.2001)

PCT

(10) International Publication Number  
**WO 01/26372 A1**

(51) International Patent Classification<sup>7</sup>: H04N 7/16, 5/00

(21) International Application Number: PCT/US00/27685

(22) International Filing Date: 6 October 2000 (06.10.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:  
60/157,968 6 October 1999 (06.10.1999) US

(71) Applicant (for all designated States except US): THOMSON LICENSING S.A. [FR/FR]; 46, quai Alphonse Le Gallo, F-92648 Boulogne Cedex (FR).

(72) Inventors; and

(75) Inventors/Applicants (for US only): ESKICIOGLU, Ahmet, Mursit [TR/US]; 8235 Lakeshore Trail, #125, Indianapolis, IN 46250 (US). DEISS, Michael, Scott [US/US]; 1103 Indian Pipe Lane, Zionsville, IN 46077 (US). DIASCORN, Jean-Louis [FR/US]; 496 Arbor Drive, Carmel, IN 46032 (US). DUFFIELD, David, Jay [US/US]; 5459 Fall Creek Road, Indianapolis, IN 46220 (US).

(74) Agents: TRIPOLI, Joseph, S. et al.; Thomson Multimedia Licensing Inc., P.O. Box 5312, Princeton, NJ 08540 (US).

(81) Designated States (national): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

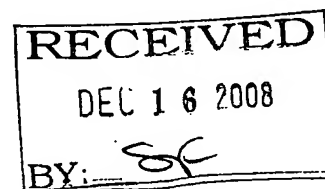
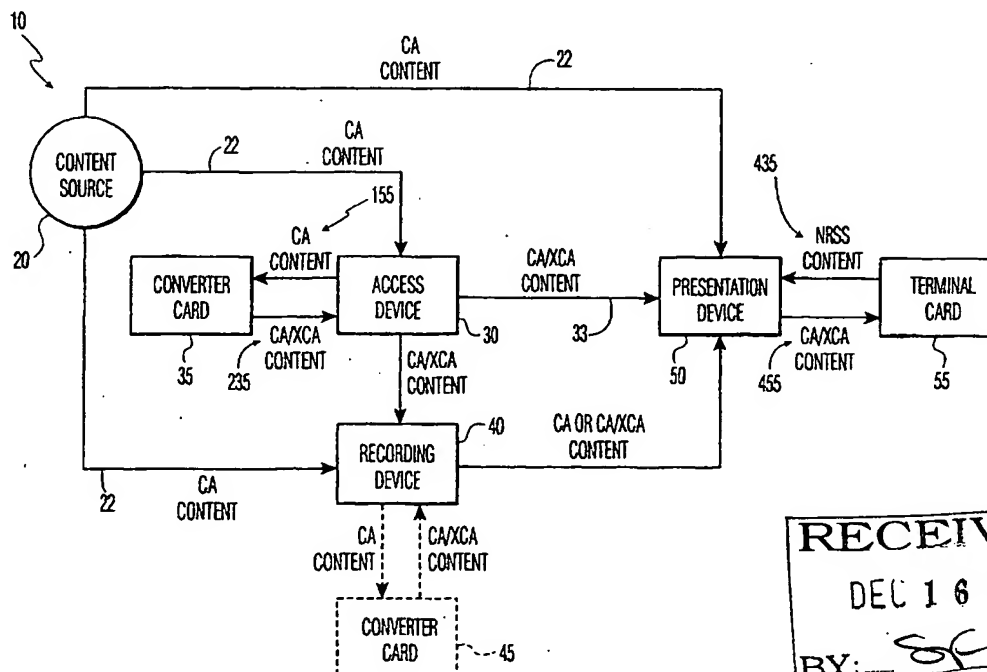
(84) Designated States (regional): ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

**Published:**

- With international search report.
- Before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments.

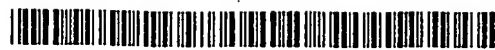
[Continued on next page]

(54) Title: METHOD AND SYSTEM FOR HANDLING TWO CA SYSTEMS IN A SAME RECEIVER



(57) Abstract: A method for enabling a security device to enable an audio/video processing system to permit access to a service, by correctly identifying the service and entitlement message packet. The audio/video transmission systems use multiple conditional access identifications.

WO 01/26372 A1



---

*For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.*

## METHOD AND SYSTEM FOR HANDLING TWO CA SYSTEMS IN A SAME RECEIVER

### Field of the Invention

5       The present invention relates generally to digital audio/video transmission systems, and more particularly to a method and system which allows a receiver in a digital audio/video transmission system to use multiple conditional access identifications.

### 10   Background of the Invention

ISO/IEC 13818-1 is an international standard that specifies the coding of one or more elementary streams of audio and video as well as other data into single or multiple streams suitable for storage and transmission. Two forms of coding are recommended: Program Stream (PS) coding and Transport Stream (TS) coding. In the coding process, Audio-Visual (A/V) streams are first compressed and packetized to obtain Packetized Elementary Streams (PES). The PS combines one or more streams of PES packets with a common time base into a single stream. The TS combines one or more programs with one or more independent time bases into a single stream. PS packets may be of variable length, and TS packets are 188 bytes in length. Each TS packet has a 4-byte header with a packet ID (PID) that identifies the type of data contained in the packet. In addition to PES packets, a TS contains Program Specific Information (PSI) tables to demultiplex and present programs. A Program Map Table (PMT) is a table that provides the mappings between the program numbers and the elements that comprise them. It includes a list of PIDs associated with each program.

25       The Advanced Television Systems Committee (ATSC) has adopted the Simulcrypt architecture for its Conditional Access (CA) system for terrestrial broadcast. In this architecture, each service is transmitted with Entitlement Management Messages (EMMs) and Entitlement Control Messages (ECMs) for a number of different proprietary systems. This way, decoders using different CA systems can decode the service using a common framework for signaling the

30

different entitlement messages. Each service is comprised of audio and video packets. Any one decoder picks out the packets it needs and ignores the others in the stream.

In a Simulcrypt based CA system, a digital audio/video processing system, such as a Digital Television (DTV) parses the PMT and extracts the service and ECM PIDs using a CA system identification (ID) obtained from the CA module. Normally, each CA module supports only one CA system, and therefore has only one CA system ID. The PIDs of the A/V packets and the PIDs of the ECMs carrying the Control Words (CWs) are sent to the CA module, which descrambles programs having proper purchase entitlements.

### Summary of Invention

The present invention permits an audio/video processing device to use two CA system IDs to parse the PMT, and the CA module to correctly identify the ECM PIDs which belong to a particular CA system. It includes a method for an A/V processing device, for example a DTV, to enable a security device to access a program by correctly identifying the packets for service and entitlement control messages. The security device is associated with the A/V processing device, which in turn is associated with a digital transmission system for data associated with a service. The method comprises extracting at least one service and entitlement message control packet identifier pair from the data and, if only one service and entitlement control message packet identifier pair is extracted, identifying the extracted pair; and, if more than one service and entitlement control message packet identifier pair is extracted, automatically selecting one of the extracted pairs according to a predefined convention.

### Brief Description of the Figures

Figure 1 illustrates a network adapted to receive content from a broadcasting source and provide copy protection using XCA and the NRSS copy protection system;

Figure 2 illustrates a block diagram of an XCA device employed within the system of Figure 1;

Figure 3 illustrates a block diagram of a converter card utilized according to an aspect of the present invention; and,

Figure 4 illustrates a block diagram of a terminal card utilized according to an aspect of the present invention.

5

#### Detailed Description of the Invention

Figure 1 illustrates a network 10 that receives content from a broadcasting source, i.e. via content source 20, and provides protection with XCA and the NRSS copy protection system (described below). The content source 20 can provide the CA content 22 of economic value, whether from tape, DVD, cable, satellite or terrestrial broadcast, for example. The content 22 typically includes A/V content, which is protected and supplied to subscribers of a private CA network. The subscribers who purchase, or are otherwise entitled to receive the content 22, are supplied with necessary keys for descrambling the content 22. According to the embodiment of Figure 1, the content source 20 can provide this CA content 22 to an access device 30, recording device 40 or presentation device 50.

Access device 30 can take the form of a set-top box. The set-top box 30 operates in conjunction with an XCA/NRSS converter card 35 to create XCA protected content from the CA content 22 which becomes part of the CA/XCA content 33. Recording device 40 can take the form of a Digital VHS (DVHS) or DVD recorder. The recording device may or may not be provided with a converter card 45 analogous to the converter card 35. Presentation device 50 can take the form of a DTV, and operate in conjunction with an XCA/NRSS terminal card 55 for descrambling CA/XCA protected content.

Extended Conditional Access (XCA) is a system for protecting MPEG2 encoded digital A/V content during transmission and storage while supporting established and new models for content distribution and sales. XCA accomplishes this task by mapping the basic controls of "playback" and "record" into viewing control. Under the XCA system, content of economic value is always scrambled, i.e., is either under the control and responsibility of the distributor or within the confines of the consumers home, e.g. local, network.

XCA allows recording of scrambled content, but only legitimate copies may be descrambled and viewed. Since non-legitimate content is not descrambled, it cannot be viewed. Non-legitimate content is that which is not an original or otherwise authorized by the copyright owner, for example.

5 XCA provides three levels of entitlements. Content that is free to distribute in unlimited fashion is "free-copy" content. Examples of this content may be broadcast television, infomercials or similar material that is advertised or supported. "Copy-once" or local view programming content can be created and viewed in a single household or local network regardless of time. However, such  
10 a copy cannot be transported to other local networks. Examples of this type of content may be sporting events or premium services. Finally, "never-copy" or immediate view programming content allows for only real-time viewing, i.e., recorded copies are not viewable. Examples of this type of content may be pay-per-view programming or other high-value content.

15 A distinct characteristic of the XCA architecture is the notion of conditional access and local protection. Local protection, or security, is the protection of content within the boundaries of a home network, after an access device, e.g. 30, receives the scrambled program, e.g. CA content 22. It specifies what a presentation device e.g. 50, has access to, and can thus  
20 convert and display protected content. Removable security devices, e.g., converter and terminal cards 35, 45, 55, perform security related functions. Content of economic value is delivered using a CA service. For example, digital satellite systems scramble video content and keys for mass distribution to their subscribers. Some subscribers may decide to purchase the content in which  
25 case they are supplied with the necessary keys for descrambling the content and viewing. Those subscribers choosing not to purchase the content are not provided access to these keys. In XCA, the descrambling keys are rebundled in a new ECM, which is protected by a unique local public key. The presentation device that receives content with local ECMs (LECMs) therefore needs to handle  
30 not only the content protected by a particular CA system, but by XCA as well.

Referring now also to Figure 2, a generic XCA Consumer Electronics (CE) device 60 suitable for use in system 10 is illustrated therein. Certain types of

device 60 have specific functionality. For example, the XCA access device 30 creates XCA protected content for CA/XCA 33, the XCA presentation device 50 descrambles XCA protected content, and the XCA recording device 40 stores and plays but cannot create or descramble XCA protected content unless it is provided with the converter card 45. Generally, the generic device 60 includes a switching unit 62, input unit 61 and a renewable or embedded security device 66, e.g. converter card 35 or 45, or terminal card 55. Depending on what type of device it is, the device 60 may also include a presentation unit 64, storage unit 68, analog output 65, decompressed digital output 67 or compressed digital output 69.

The digital input unit 61 generally comprises circuitry and software needed to acquire a digital signal, for instance a demodulator. The compressed digital output 69 uses circuitry and software to issue an MPEG2 digital signal, for instance a modulator. Security device 66 handles CA functions and XCA functions, and is able to transform the type of the content. It is the only element of the model that outputs in digital format a transformed content. As set forth, the security device 66 may take the form of the converter card 35 or 45, or terminal card 55. The converter cards 35 and 45 support functionality such as (i) checking CA entitlements; (ii) control word (CW) recovery; and (iii) content descrambling. It generates the Triple Data Encryption Standard (TDES) keys, re-scrambles the content, and encrypts the LECMs using its public key. The terminal card 55 supports functionality, such as checking XCA entitlements. It descrambles the content using the CWs of the LECMs, and then re-scrambles the content following the requirements of the XCA NRSS interface protection system. Block diagrams of an exemplary converter card 35 and terminal card 55 are illustrated in Figures 3 and 4, respectively. The storage unit 68 stores content in, and reads content from, non-volatile memory. It does not transform the type of the content unless provided with a converter card 45, in which case it also acts as an access device. A hard disk is a typical internal storage unit. Digital Versatile Disc (DVD) players and Digital Video Tape Recorders such as DVHSs are typical CE devices with removable storage. The presentation unit 64 decodes the MPEG2 content, and presents it to the user in an analog or

decompressed digital form. It may descramble an NRSS stream using NRSS descrambler 64', decode a digital stream using MPEG decoder 64'', and perform digital to analog conversion using digital to analog converter (DAC) 64'''. The final outcome may be a physical signal such as sound or an analog electrical signal. TV display and analog output of a hi-fi amplifier are typical examples. The switching unit 62 routes content within the device 60. Its function is limited to routing only; it does not transform the type of the content.

The XCA system is designed to protect the NRSS interface connecting an XCA terminal card 55 to a presentation device 50. NRSS interface protection is not required in access device 30 as the content is CA/XCA content.

The procedure for establishing an XCA protected NRSS interface involves: authenticating the presentation host device 50; establishing a shared secret key that is unique to a particular presentation device 50/terminal card 55 pair; creating shared keys for content protection; and scrambling content returning to the host 50 with Data Encryption Standard (DES) and the shared keys.

The Local Entitlement Control Message (LECM) may be contained in one or more sections which may be variable in length with the syntax of Table 1. The beginning of a section can be indicated by a pointer field in the packet payload.



Table 1

Syntax	No. of Bits	Mnemonic
Local_Entitlement)Control_Message{		
Table_id	8	0x80 or 0x81
Section_syntax_indicator	1	'1'
Private_indicator	1	'1'
Zero	2	'00'
Private_section_length	12	Uimbsbf
Table_id_extension(){		
Reserved	6	'000000'
LECM_type	2	'10'
Protocol_version	8	Uimbsbf
}		
Reserved	2	'11'
Version_number	5	'00000'
Current_next_indicator	1	'1'
Section_number	8	0x00
Last_section_number	8	0x00
XCA_indentifier	256	Uimbsbf
Local_source_id	64	Uimbsbf
Reserved	5	Uimbsbf
Copy_protect_enable	1	Uimbsbf
XCA_view_flag	2	Uimbsbf
Time_code	32	Uimbsbf
Source_sequence_number	32	Uimbsbf
XCA_descriptor	424	Uimbsbf
Padding_bytes	508	Uimbsbf
Integrity_check	32	Uimbsbf
CRC_32	32	Rpchof

where,

**Table\_id**--This 8-bit field identifies the Entitlement Control Message that this section belongs to. It shall be set to either 0x80 or 0x81. When at least one bit changes in the LECM section, the table\_id shall toggle.

**Section\_syntax\_indicator**--This 1-bit field shall be set to '1'. It denotes that the section follows the generic section syntax beyond section length field.

**Private\_indicator**--This 1-bit field shall be set to '1'.

**Private\_section\_length**--This 12-bit field specifies the number of remaining bytes in this section, starting immediately following the private\_section\_length field, and including the CRC\_32.

**LECM\_type**--This 2-bit field indicates the type of information carried by the LECM. '10' means that it carries a Control Word.

**Protocol\_version**--An 8-bit unsigned integer field whose function is to allow, in the future, this table to carry parameters that may be structured differently than those defined in the current protocol. At present, only one protocol is defined. When Protocol\_version = 0x00, only a single control word pair is used for the entire program, and similarly, the access criteria is defined for the entire program (i.e., no stream-level protection allowed). In this case, all streams of the event shall be scrambled with the same control word, and shall use the same access criteria. When Protocol\_version > 0x01, values of protocol\_version greater than 0x00 may only be processed by decoders designed to accommodate the later version of the protocol as they become deployed.

**Version\_number**--This 5-bit field is reserved and shall have a value of '00000'. Future implementation can use this field if necessary.

**Current\_next\_indicator**--This 1-bit indicator is always set to '1' for a LECM; the LECM sent is always currently applicable.

**Section\_number**--This 8-bit field contains the number of the private section. The section number of the first section in a private table shall be 0x00. The section number shall be incremented by 1 with each additional section belonging to this private table.

**Last\_section\_number**--This 8-bit field specifies the number of the last section of the private table of which this section is a part.

**XCA\_identifier**--This 256-bit field contains a unique XCA identifier. The

identifier has ASCII values of "Copyright: (C) 1999 TMM". Quotation marks are not included. Each ASCII character is assigned one byte of storage. Characters are left-justified in this field. Unassigned field values are set to 0x00.

**Local\_source\_id**--This 64-bit field contains the XCA device ID of the security device that generated this LECM.

**Copy\_protect\_enable**--This 1-bit field shall indicate the presence of a content protection mechanism for one or more streams of the program material that is delivered out of the presentation device. The purpose of this flag is to provide a means to detect fault indication for the user and shall not be used to enforce copy protection. The value of this field is set to '1' if the protection for at least one stream is enabled.

**XCA\_view\_flag**--The value of this 2-bit field shall be determined by the authority that manages protection of the program content prior to conversion to XCA protection. This value shall be compared with the value of the XCA\_view\_flag in the XCA\_descriptor. In case of a discrepancy, the protected XCA\_view\_flag shall be used to enforce viewing rights within the security processor of an XCA Presentation Device. The semantic shall be as follows:

XCA\_view\_flag='00': XCA content is not restricted. View anywhere, any time. XCA\_view\_flag='01': XCA reserved. XCA\_view\_flag='10': XCA content is restricted to viewing any time within the local network. XCA\_view\_flag='11': XCA content is restricted to viewing "now" within the local network.

**Time\_code**--If the time source is known and secure, this field contains the number of seconds that has transpired since 12 am January 6, 1980 UTC (mod  $2^{32}$ ). If the time source is not known and secure, this field shall be coded as all 0's.

**Source\_sequence\_number**--This 32-bit field contains the current value of the cryptoperiod counter of the converter module that created the LECM.

**Padding\_bytes**--The number of bytes needed to make the total length of the secure part of the LECM 128 bytes (128-65). The padding\_bytes are randomly chosen.

**Integritycheck**--This 32-bit number field contains a value that verifies that

the content of the decrypted payload is valid. It is used to ensure the encryption and decryption processes are performed properly.

- CRC-32**--This 32-bit field contains the CRC value that ensures a zero output from the registers in the decoder defined in Annex A of ISO/IEC 13818-1
5. "MPEG2Systems" after processing the entire LECM section. This value shall be calculated after the data have been encrypted.

Each converter card 35 supports a transformation from CA protected content to XCA protected content and has a 32-bit cryptoperiod counter. A cryptoperiod is defined as the period during which a stream or a program is

10 scrambled with one particular key. For each new cryptoperiod, i.e., control word change, the converter module shall increment its cryptoperiod counter by 1. If, for example, a program includes three streams with different cryptoperiods, the counter is incremented at the beginning of each cryptoperiod for each stream. Protected against external access, this counter cannot be reset or decreased.

15 The initial value of the cryptoperiod counter is 0.

Once the converter card 35 determines that the access to the content is legitimate, it uses the following information to build the LECM: odd and even CWs; Copy Control Information (CCI); and Copy Protection (CP) status, e.g., one of the three possible states "view freely", "view locally", or "view now".

20 The transformation from CA protected content to XCA protected content includes the following processes: the converter card 35 assigns its XCA\_ID to local\_source\_id; the converter card 35 sets copy\_protect\_enable to 1 if the content is of type "view now", otherwise copy\_protect\_enable is set to 0; the converter card 35 assigns the current value of the cryptoperiod counter to

25 source\_sequence\_number; and, the converter card assigns a hash value computed on the secure-part of the LECM to integrity\_check.

The hash method is as follows according to an aspect of the present invention:

$$\begin{aligned}
 C[0] &= M[0] \oplus M[4] \oplus \dots \oplus M[4 \times (n/4)] \\
 C[1] &= M[1] \oplus M[5] \oplus \dots \oplus M[4 \times ((n-1)/4) + 1] \\
 C[2] &= M[2] \oplus M[6] \oplus \dots \oplus M[4 \times ((n-2)/4) + 2] \\
 C[3] &= M[3] \oplus M[7] \oplus \dots \oplus M[4 \times ((n-3)/4) + 3]
 \end{aligned}$$

30

where,  $M[i]$  represents the  $i^{\text{th}}$  byte of the message to encrypt, the first byte of the sequence has index 0; and,  $C[i]$  represents the  $i^{\text{th}}$  byte of the integrity\_check field, the first byte of the field has index 0.

The secure part of the LECM is encrypted using RSA-1024. The  
5 encryption key is the free viewing public key  $K_{\text{pub\_free}}$ , if the content is of "free viewing" type, otherwise it is the converter card's public key  $K_{\text{pub\_i}}$ . Finally, the converter card calculates CRC\_32 after encrypting the secure part of LECM.

Referring again to Figure 3, therein is illustrated a block diagram of an exemplary converter card 35. Converter card 35 includes a CA system 100 and  
10 an XCA system 200. The CA system 100 generally includes: an ISO-7816 link device 110 communicable with the host device, e.g. access device 30, via the link 37; CA operational Software (SW) 120; ECM and EMM extractors 130, 140; and Triple Data Encryption Standard (TDES) device 150. An input 155 for receiving CA content from the host is provided and supplied to TDES device  
15 150, and ECM and EMM extractors 130, 140. The TDES device 150 further includes an output 160. The XCA system 200 generally includes XCA operational software 220 and ECM replacement module 230. The ECM replacement module 230 is communicable with the TDES conversion module 150 via the output 160. The ECM replacement module 230 is further provided  
20 with an output 235 for returning XCA content to the host.

Terminal card 55 supports a transformation of XCA protected content to NRSS content. For this purpose, the terminal card 55 holds a record for each converter card 35(i) linked to it. This record contains the following fields: the XCA\_ID of the converter card 35(i); the private key  $K_{\text{priv\_i}}$  of the converter card  
25 35(i); and, the most recent value of the source\_sequence\_number  $SSN_i$  received from the converter card 35(i). The transformation of XCA protected content to NRSS content includes: if the value of CRC\_32 does not match with the value computed from LECM, then the terminal card 55 cancels the transformation. If the status of the content defined by XCA\_view\_flag corresponds to "free  
30 viewing" type, then the decryption key is the free viewing private key  $K_{\text{priv\_free}}$ . The terminal card 55 decrypts the secure part of LECM using RSA-1024. From

the unencrypted local\_source\_id, the terminal card 55 identifies the issuing converter card 35. If the terminal card 55 does not yet have the corresponding private key, i.e., if the terminal card 55 does not have a record whose first field is equal to the value of local\_source\_id, then it stops the transformation, and  
5 initiates a request for the private key. Otherwise, the terminal card 55 decrypts the secure part of LECM with RSA-1024 using the private key associated with the converter card 35 identified by local\_source\_id. If the value of XCA\_view\_flag in the unencrypted part does not match with the value of XCA\_view\_flag in the XCA descriptor, then the terminal card 55 cancels the  
10 transformation. If the content corresponds to the "view now" type, then the terminal card 55 ensures that there is no replay using two checks. If a secure time source is not available for the host, then the first check is omitted. In the first check, the terminal card 55 compares time\_code with the host time received from the presentation device 50 using an NRSS command. If the difference is  
15 not more than a predetermined amount, e.g. five minutes, then the terminal card 55 compares SSNi with source\_sequence\_number. Otherwise, it cancels the transformation. In the second check, if SSNi is less than source\_sequence\_number, then the terminal card 55 updates the corresponding SSNi, and descrambles the content using the CWs in the LECMs. Otherwise, it  
20 cancels the transformation. If the content does not correspond to the "view now" type, then the terminal card 55 descrambles the content using the CWs in the LECMs. The terminal card 55 passes the contents of the CCI field to the NRSS module 300 for NRSS protection purposes. Finally, the terminal card 55 informs the NRSS module 300 of each new cryptoperiod occurrence.

25 In another transformation, XCA protected content is transformed to clear content. This transformation is similar to transforming XCA protected content to NRSS content, where noteworthy differences are: that the clear content is directly passed to the switching unit 62 of a device 60 for example; and, that the CCI is directly passed to the host processor.

30 Referring again to Figure 4, therein is illustrated a block diagram of an exemplary terminal card 50. Generally, the terminal card 50 includes a CA system 400, and an XCA system 300. The CA system 400 generally includes:

an ISO-7816 link device 410 communicable with the host device, e.g. presentation device 50, via the link 57; CA operational software (SW) 420; ECM and EMM extractors 430, 440; and Triple Data Encryption Standard (TDES) descrambling device 450. Input 455 for receiving CA/XCA content from the host is provided and supplied to TDES device 450, and ECM and EMM extractors 430, 440. The TDES device 450 further includes an output 460. The XCA system 300 generally includes XCA operational software 320; NRSS copy protection operational software (SW) 340; and NRSS copy protection (CP) module 350. The NRSS copy protection (CP) module 350 is communicable with the TDES descrambling module 450 via the output 460. The NRSS copy protection (CP) module 350 is further provided with an output 435 for returning NRSS content to the host.

Terminal cards 55 exchange data with the host device 50 to complete their tasks. This communication can be effected using NRSS EIA-679B compliant commands, for example. In accordance with the applicable NRSS specification, the host monitors the card status periodically to determine what operations need to be performed.

The National Renewable Security Standard (NRSS) provides a means for renewable security to be employed with digital Consumer Electronics (CE) devices such as DTV receivers and digital VCRs. The security functionality is thus separated from navigational devices. When an NRSS security device, such as terminal card 55, receives protected content from its host device, such as presentation device 50, it descrambles it and sends it back to the host device. As the content is in-the-clear before it leaves the security device, it needs to be protected across the interface. The NRSS standard also defines a framework for encryption-based copy protection systems.

According to the NRSS specification, hosts and terminal cards may be manufactured with support for one or more NRSS copy protection systems. These systems are identified by unique Copy Protection (CP) system IDs. A negotiation can be used between a terminal card 55 and its host device 50 to determine which systems are implemented. As part of the terminal card 55 initialization, the host 50 informs the terminal card 55 about the NRSS copy

protection systems it supports. If an XCA NRSS copy protection system is included in this set, the terminal card 55 sends back the CP system ID with its configuration which also includes the CA system ID. Looking at this configuration, the host 50 realizes that both XCA and a particular CA system are supported by the terminal card 55, and subsequently parses the PMT using both the XCA system ID and CA system ID. For each new program, the card 55 obtains service and ECM PIDs from the host. According to an aspect of the invention, the XCA CA system ID is stored in host devices supporting the XCA copy protection system as it is not a confidential piece of data, and does not require secure storage.

By construction, the terminal card 55 processes both CA and XCA streams coming from various sources including broadcaster head-end and playback devices in the home network. Depending on the content received, the host e.g. presentation device 50, may send either one or two pairs of {Service PID, ECM PID} to the terminal card 55. Three possibilities may exist: (1) Only one pair is sent; {Service PID, ECM PID} which contains the LECM PID; (2) Only one pair is sent; {Service PID, ECM PID} which contains the CA ECM PID; or, (3) Two pairs are sent; where one pair contains the LECM, the other the CA ECM PID. Hence, there is a need to differentiate between CA ECMs and LECMs. Two exemplary cases are provided.

Case (a): Where two pairs are provided - The first {Service PID, ECM PID} pair is defined to be a predetermined one of the PIDs, e.g. the LECM PID or CA ECM PID by convention.

Case (b): Where only one pair is received - The terminal card detects LECMs by checking their syntax, such as was discussed in relation with Table 1. According to another aspect of the invention, two fields that may be used for this purpose are LECM\_type and XCA\_identifier. The former indicates what the transport packet carries, while the latter provides a unique identification for the XCA LECM.

For example, consider a program with the following service PIDs: (1) Video PID: 100, and (2) Audio PID: 101. These two elementary streams are protected with the same key. The descrambling keys are carried in ECMs



protected by two CA systems (there may be more than two CA systems): (1) CA system #1 ECM PID: 180, and (2) CA system #2 ECM PID: 181. Assume the ECM for CA system #1 is converted to and replaced by, an LECM with PID 182. Now, the host device will send two sets of (service PID, ECM PID) pairs to the card as is characterized by Table 2.

Table 2

Service PID	ECMPID
100	182
101	182
100	181
101	181

The PID 182 will be identified to be the PID for LECMs where the first of the pairs was set to be the LECM PIC by convention.

Claims

1. A method for an audio/video processing device to enable a security device to access a service, the method comprising:

5 extracting service and entitlement control message packet identifier pairs from data associated with said service and automatically identifying one of the extracted pairs according to a predefined convention.

10 2. The method according to claim 1, wherein the predefined convention is dependent upon an order in which the pairs are sent to the security device.

15 3. The method of Claim 1, wherein each of the received pairs is either associated with a conditional access (CA) system or extended conditional access (XCA) system.

4. A method for an audio/video processing device to enable a security device to access a service, the method comprising:

extracting the service and entitlement control message packet identifier pairs from data associated with said service; and,

20 if only one service and entitlement control message packet identifier pair is extracted, identifying the extracted pair; and,

if more than one service and entitlement control message packet identifier pair are extracted, automatically identifying at least one of the extracted pairs according to a predefined convention.

25

5. The method of Claim 4, wherein the predefined convention is dependent upon an order in which the pairs are extracted.

30 6. The method of Claim 5, wherein each of the received pairs includes either a conditional access entitlement control message identifier or a local entitlement control message identifier.

7. The method of Claim 6, wherein each of the received pairs further includes a service identifier.

8. The method of Claim 6, wherein the predefined convention defines a first of the pairs to be received to include the service identifier and local entitlement control message identifier.

9. The method of Claim 4, wherein at least a portion of the data is secured using one of a plurality of conditional access systems.

10. The method of Claim 9, wherein at least one of the conditional access systems is associated with a broadcaster of the program and at least a second of the conditional access systems is associated with an access device, communicable with the presentation device.

11. The method of Claim 10, wherein the presentation device is a digital television, and the access device is a set-top box in combination with a second security device.

12. The method of Claim 4, further comprising:

the security device communicating interface protection related information and conditional access related information to the audio/video processing device; and,

the audio/video processing device parsing a program map table using the communicated conditional access information and stored conditional access information;

wherein the program map table associates packet identifiers with corresponding service information.

13. The method of Claim 12, wherein the security device uses packet identifiers to identify which of the packets contains entitlement control message data suitable for descrambling the data indicative of the program.

14. The method of Claim 13, wherein at least some of said entitlement control messages are local entitlement control messages which include at least a field for identifying and LECM and a field for conditional access identification, and  
5 said proper processing comprises descrambling said service by accessing an appropriate key in said data using information included in at least one of said field for identifying and LECM and said field for conditional access identification.
15. The method according to claim 9, wherein at least one portion of the data  
10 is indicative of at least one program.
16. The method according to claim 4, wherein the data is communicated via a digital transmission system.

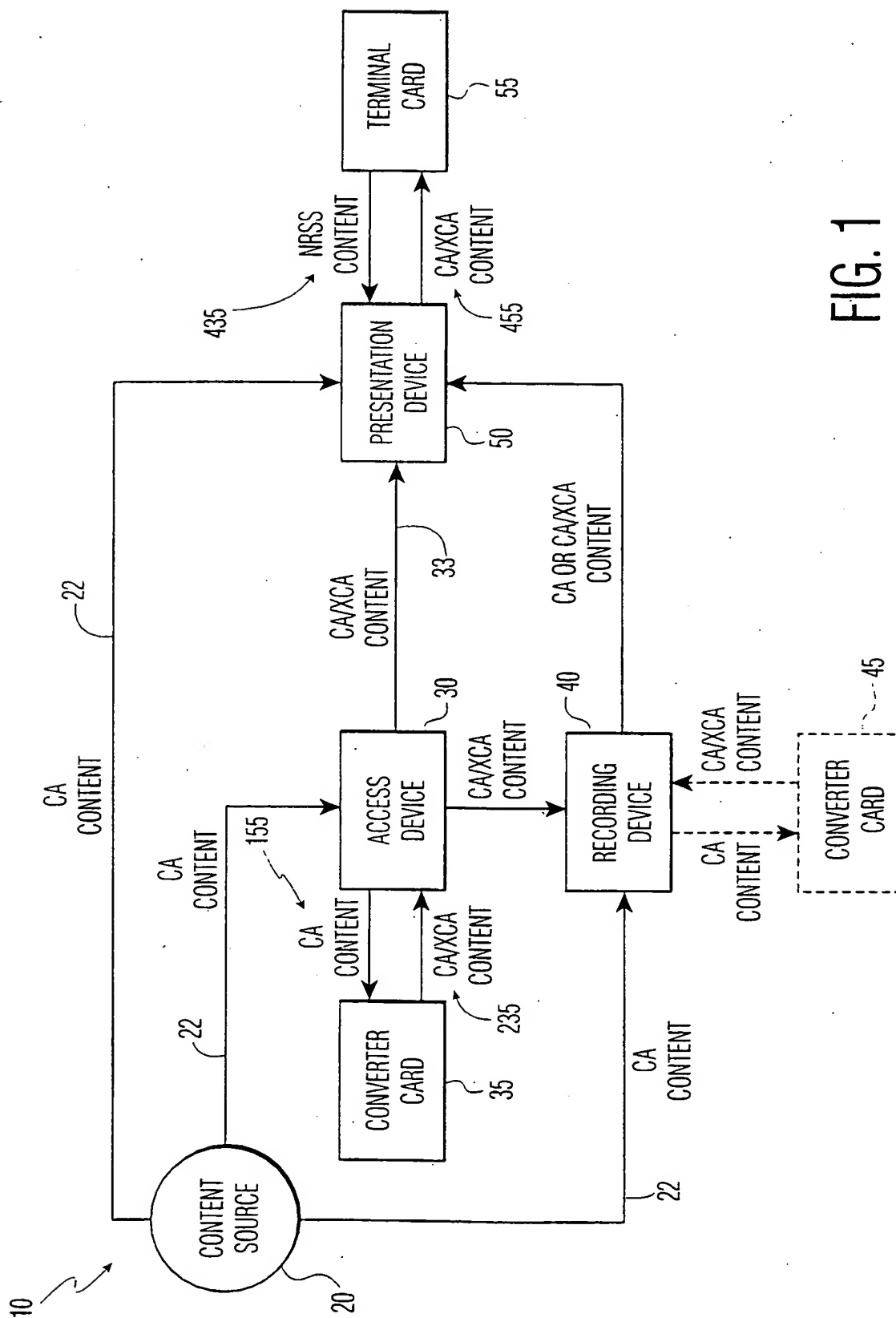
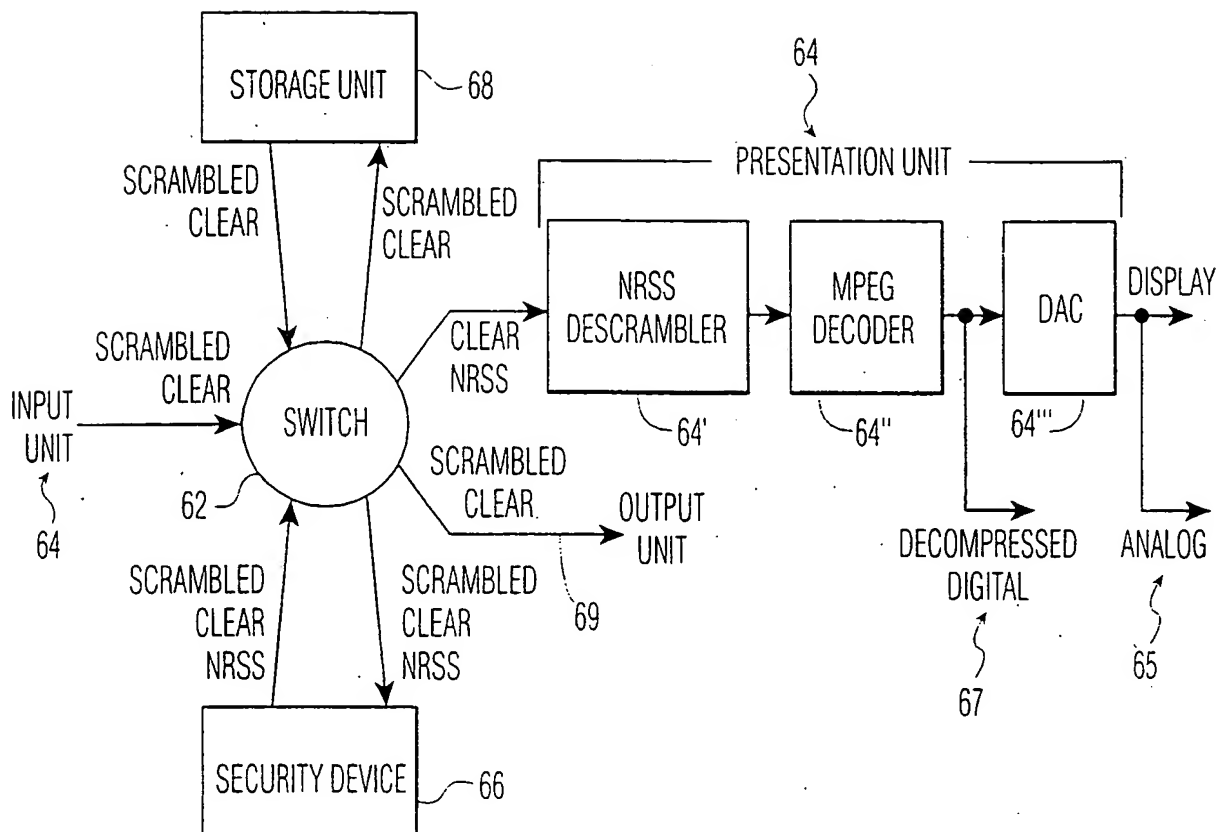


FIG. 1

2/3



## TYPES OF CONTENT:

SCRAMBLED: CA AND XCA CONTENT; CLEAR: UNSCRAMBLLED MPEG TRANSPORT STREAM; NRSS: SINGLE DES SCRAMBLED TRANSPORT STREAM. THIS CONTENT IS INDISTINGUISHABLE FROM SCRAMBLED CONTENT WHEN THE DESCRAMBLING KEY(S) ARE NOT AVAILABLE.

FIG. 2

3/3

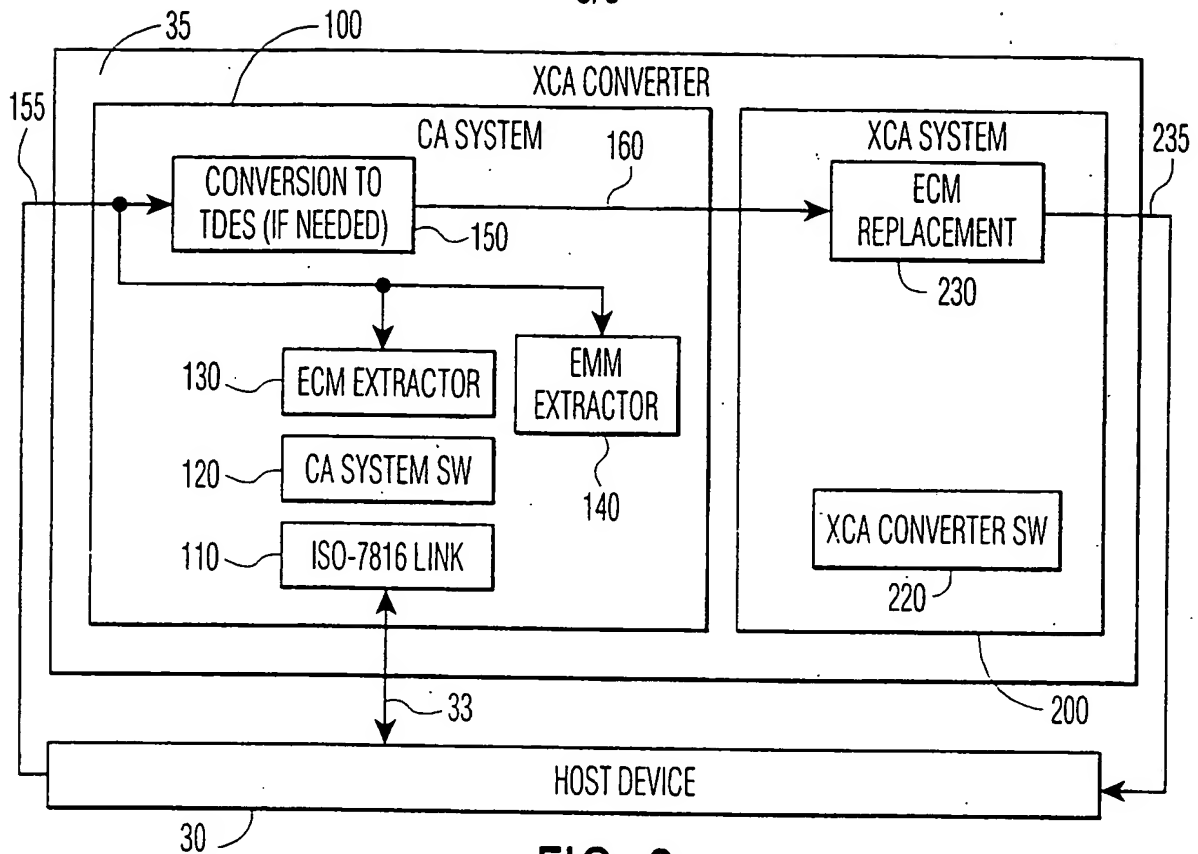


FIG. 3

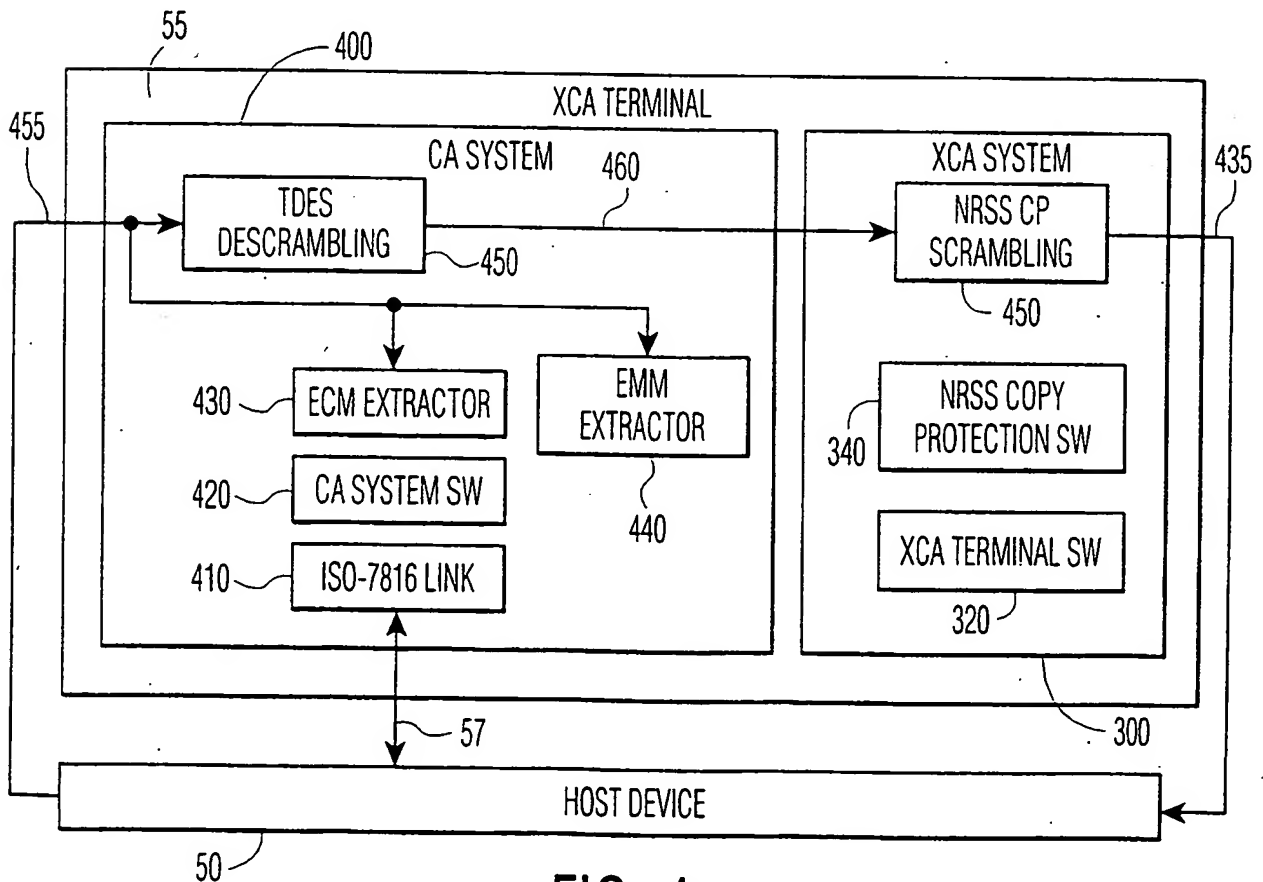


FIG. 4

# INTERNATIONAL SEARCH REPORT

In' tional Application No

PCT/US 00/27685

**A. CLASSIFICATION OF SUBJECT MATTER**  
 IPC 7 H04N7/16 H04N5/00

According to International Patent Classification (IPC) or to both national classification and IPC

**B. FIELDS SEARCHED**

Minimum documentation searched (classification system followed by classification symbols)

IPC 7 H04N

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal, COMPENDEX, INSPEC, IBM-TDB

**C. DOCUMENTS CONSIDERED TO BE RELEVANT**

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X A	US 5 420 866 A (WASILEWSKI ANTHONY J) 30 May 1995 (1995-05-30) column 1, line 14 -column 7, line 7  figures 1-8  ---	1,4,9  2,3,5-8, 10-16
P,X	WO 00 56068 A (THOMSON LICENSING S A ;DEISS MICHAEL SCOTT (US); ESKICIOGLU AHMET) 21 September 2000 (2000-09-21) page 2, line 14 - line 29 page 4, line 4 -page 5, line 14 figures 1-8  ---	1,3
A	EP 0 858 184 A (NDS LTD) 12 August 1998 (1998-08-12) column 1, line 12 -column 7, line 20 figures 1-5  ---  -/--	1-16



Further documents are listed in the continuation of box C.



Patent family members are listed in annex.

\* Special categories of cited documents :

- \*A\* document defining the general state of the art which is not considered to be of particular relevance
- \*E\* earlier document but published on or after the international filing date
- \*L\* document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- \*O\* document referring to an oral disclosure, use, exhibition or other means
- \*P\* document published prior to the international filing date but later than the priority date claimed

- \*T\* later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
- \*X\* document of particular relevance: the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
- \*Y\* document of particular relevance: the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
- \*Z\* document member of the same patent family

Date of the actual completion of the international search

30 January 2001

Date of mailing of the international search report

06/02/2001

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2  
 NL - 2280 HV Rijswijk  
 Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,  
 Fax: (+31-70) 340-3016

Authorized officer

Tito Martins, J



# INTERNATIONAL SEARCH REPORT

International Application No

PCT/US 00/27685

## C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	<p>"FUNCTIONAL MODEL OF A CONDITIONAL ACCESS SYSTEM" , EBU REVIEW-TECHNICAL, BE, EUROPEAN BROADCASTING UNION. BRUSSELS, NR. 266, PAGE(S) 64-77            XP000559450            ISSN: 0251-0936            the whole document</p>	1-16
A	<p>KRAMER D: "WUNDERKISTE DES DIGITALEN FERNSEHENS" , BULLETIN SEV/VSE, CH, SCHWEIZERISCHER ELEKTROTECHNISCHER VEREIN, ZÜRICH, VOL. 88, NR. 3, PAGE(S) 27-30 XP000885105            ISSN: 0036-1321            page 27-28</p>	1-16

# INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No

PCT/US 00/27685

Patent document cited in search report		Publication date	Patent family member(s)	Publication date
US 5420866	A	30-05-1995	AU 687844 B	05-03-1998
			AU 7220994 A	17-10-1995
			CA 2186368 A,C	05-10-1995
			JP 2940639 B	25-08-1999
			JP 9511369 T	11-11-1997
			WO 9526597 A	05-10-1995
WO 0056068	A	21-09-2000	AU 3629100 A	04-10-2000
EP 0858184	A	12-08-1998	IL 120174 A	28-10-1999
			GB 2322030 A,B	12-08-1998